UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

MF

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/023,672	02/13/98	SCHEIDT E	STS-119

LMC1/0727

RABIN AND CHAMPAGNE
1101 14TH STREET NW
SUITE 500
WASHINGTON DC 20006

EXAMINER	
DARROW, J	
ART UNIT	**PAPER NUMBER**
2767	13

DATE MAILED: 07/27/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

U.S. G.P.O. 2000 ; 465-188/25266

Office Action Summary	Application No. **09/023,672**	Applicant(s) **Scheldt et al.**	
	Examiner **Justin T. Darrow**		Group Art Unit **2767**

☒ Responsive to communication(s) filed on *5 Jun 2000*

☒ This action is **FINAL.**

□ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *three* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) *1-69* is/are pending in the applicat

Of the above, claim(s) ______ is/are withdrawn from consideration

□ Claim(s) ______ is/are allowed.

☒ Claim(s) *1-69* is/are rejected.

□ Claim(s) ______ is/are objected to.

□ Claims ______ are subject to restriction or election requirement.

Application Papers

□ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

□ The drawing(s) filed on ______ is/are objected to by the Examiner.

☒ The proposed drawing correction, filed on *18 Feb 2000* is ☒ approved □ disapproved.

□ The specification is objected to by the Examiner.

□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

□ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

□ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

□ received.

□ received in Application No. (Series Code/Serial Number) ______ .

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______

☒ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

□ Notice of References Cited, PTO-892

□ Information Disclosure Statement(s), PTO-1449, Paper No(s). ______

☒ Interview Summary, PTO-413

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

1. Claims 1-69 have been examined.

Drawings

2. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

3. The proposed drawing correction and/or the proposed substitute sheets of drawings, filed on 02/18/00 have been acknowledged.

Response to Arguments

4. Applicant's arguments filed 06/05/00 have been fully considered but they are not persuasive.

As per claims 1, 5, 35, 36, 38, 39, and 66-69, Hirsch clearly states a plurality of key split generators (see "multibit container location" in column 1, lines 57-58) for generating cryptographic key splits (see "unique sequence of random number values" in column 1, lines 58-59); and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key (see "scrambler" in column 1, lines 54-55); in which each of the key splits generators includes means for generating key splits from seed data (see "stored input binary value" in column 1, line 62). Thus, in this disclosure the key splits are the individual bits of the "stored input binary number rearrang[ed] . . . as a function of the random number values," (see column 1, lines 62-64) and the their respective complements (see column 3, lines 65-68); the seed data of which the key splits are generated are the individual bits of the stored input binary number (see column 1, lines 62-64) and the "different one[s] of a unique sequence of random number values (see column 1, lines 57-59); and the key split randomizer for randomizing the key splits to produce a cryptographic key is "exclusive or means for performing an exclusive or of the numeric value of bit position of the input binary bit applied as an input . . . with the random number stored in the container . . . [in which] the least significant bit of the result . . . defines if the input binary bit or its complement is to be applied as an output of the container" (see column 3, lines 60-68 and column 4, lines 1-10). The applicants' assertion that Hirsch discloses "a plurality of containers in a single scrambler array which together receive a single serially-shifted pseudorandom sequence generated from a single seed" is not correct. The containers represent key split generators which contain key splits (see column 1, lines 57-59) generated from different seeds (see column 2, lines 19-34). The applicants' assertion that Hirsch discloses "taking a single 32-bit scrambled value, and mapping 8-bit segment of that value according to a stored, predetermined table, to generate a key" is also not correct. There is no predetermined table disclosed. Table 204 represented in column 4, lines 50-68 and column 5, lines 1-13 is the result of the randomization depicted in figure 1C for the specific embodiment that Hirsch discloses.

As per claims 3 and 37, Albert et al. disclose a random number generating system that picks, at a random point in time, a value from another system generating different random numbers as a function of time (see column 1, lines 51-67 and column 2, lines 1-2). This can readily be combined with random key split generator of Hirsch (see column 2, lines 23-29). In response to applicants' argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation to combined the references is to increase the quality of random numbers with respect to their predictability and their functional link (see column 1, lines 66-67 and column 2, lines 1-2).

As per claims 5 and 39, in response to applicants' argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation to combine the references is to ensure unguessability (see column 3, lines 2-7).

As per claims 6, 7, 9-11, 13-16, 40, 41, 43-45, and 47-50, although Ming et al. do not explicitly disclose the feature of key splits, these features are deemed to be inherent to the Ming et al. system as lines 1-43 of column 4 show that the seed values are used to descramble the frames within the receiving unit. The Ming et al. system would be inoperative if the seed values were not key splits. There is no misunderstanding of the claimed invention. Ming et al. suggestion that the seed values are key splits is within the scope of "key splits generated using the seed value" in which generating is specifically equating. As discussed above, Hirsch provides embodiments of other methods of generating. Ming et al. disclosure of "generating and storing the seed value" is the same as "generating a key split based on static based on static data" recited in claims 6 and 40 because the seed value is time-independent (see column 4, lines 4-7).

As per claims 7 and 41, Ming et al. do disclose updating the static data (see "incrementing the first frame counter" in column 4, lin 18). The frame count value is within the scope of interpretation of static data as recited in claims 7 and 41. The discussion of Ming et al. of "generating the next seed value" is equivalent to "updating static data" recited in claims 7 and 41.

As per claims 9 and 43, Ming et al. specifically state that access codes are required along with the seed values for decoding (see column 6, lines 53-58). Since these access codes can be combined to obtain different programing (see column 6, lines 53-58), they fall within the scope of key splits. Ming et al. also suggest token entry of the access codes (see column 6, lines 43-47 and column 10, lines 27-34).

As per claims 10 and 44, Ming et al. state a means for reading (see "subscriber's decoder apparatus" column 7, lines 17-21) the label data (see "subscriber's user address" column 7, lines

17-21) from a storage medium (see "prestored user address" column 7, line 19). As explained above, the feature of randomizing with other key splits is taught by Hirsch.

As per claims 11 and 45, Ming et al. describe label data that includes user authorization data (see column 7, lines 11-22). Since the authorization data along with other data is required for decoding (see column 7, lines 26-30), it falls withing scope of a key split. Ming et al. also suggest token entry of the access codes (see column 6, lines 43-47 and column 10, lines 27-34).

As per claims 13 and 47, Ming et al. elaborate that the pseudorandom number is derived from seeds and the access control data (see column 14, lines 30-67; column 15, lines 1-3; and column 15, lines 40-60). The "label data" is the 8-bit concatenation of the random data and the access code data. As a result, this is equivalent to "generating a pseudorandom sequence based on label data" as recited in claims 13 and 47.

As per claims 14 and 48, Ming et al. disclose generating a split based on label data (see column 6, lines 26-29) and organization data (see column 6, lines 59-65). Since these access codes and classifications can be combined to obtain different programing (see column 6, lines 53-65), they fall within the scope of key splits. Ming et al. also suggest token entry of this data (see column 6, lines 43-47 and column 10, lines 27-65).

As per claims 15 and 49, Ming et al. discuss generating a split based on label data and static data (see column 4, lines 4-7). Although Ming et al. do not explicitly disclose the feature of key splits, these features are deemed to be inherent to the Ming et al. system as lines 1-43 of column 4 show that the seed values are used to descramble the frames within the receiving unit.

The Ming et al. system would be inoperative if the seed values were not key splits. As explained above, Hirsch describes the randomizing key split combiner that can be combined with the teaching of Ming et al.

As per claims 16 and 50, Ming et al. do disclose updating the static data (see "incrementing the first frame counter" in column 4, line 18). The frame count value is within the scope of interpretation of static data as recited in claims 16 and 50. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Ming et al. teach the motivation of synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4).

As per claims 8 and 42, Ming et al. elaborate that the frame count can be set equal to integer values from 1 to N, the size of the frame sets (see column 3, lines 65-67 and column 4, lines 1-43). Since the frame count value is incremented, this value may assume the magnitude of different divisors of the value N. As mentioned above, Hirsch teaches the feature of a random key split.

As per claims 12 and 46, Ming et al. discuss that the pseudorandom number is derived from seeds and the access control data (see column 14, lines 30-67 and column 15, lines 1-3).

As per claims 17 and 51, Ming et al. elaborate that the frame count can be set equal to integer values from 1 to N, the sized of the frame sets (see column 3, lines 65-67 and column 4, lines 1-43). Since the frame count value is incremented, this value may assume the magnitude of different divisors of the value N.

As per claims 18 and 52, Anshel et al. describe generating a key split from maintenance data (see "s = 1, 2, 3, . . . denote the state of the user" in column 8, lines 8-15).

As per claims 20 and 54, Anshel et al. specify generating a pseudorandom sequence (see "Upon receiving the inputs k, s, 40, the Zeta Pseudorandom Number Generator ZPNG 41 outputs zeta code . . ." in column 8, lines 15-17).

As per claims 21 and 55, Anshel et al. do not explicitly disclose the feature of using previous maintenance data and current maintenance data. However, this feature is deemed to be inherent to the Anshel et al. system as lines 26-28 of column 8 show that these values are related. The Anshel et al. system would be inoperative if the key split were not based on previous maintenance data and on current maintenance data.

As per claims 22 and 56, Anshel et al. do disclose generating a key split based on the maintenance data (see "s" in column 8, line 16) and static data (see "k(0)" in column 8, line 16).

As per claims 23 and 57, an incremented state value is within the scope of "updating the static data" as recited in claims 23 and 57. As mentioned above Anshel et al. describe generating a key split based on maintenance data.

As per claims 24 and 58, Anshel et al. do suggest updating the static data including modifying the prime number divisor of the static data (see "e = a.k" in column 11, line 45).

As per claims 19 and 53, Hirsch clearly states a plurality of key split generators (see "multibit container location" in column 1, lines 57-58) for generating cryptographic key splits (see "unique sequence of random number values" in column 1, lines 58-59); and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key (see "scrambler" in column 1, lines 54-55); in which each of the key splits generators includes means for generating key splits from seed data (see "stored input binary value" in column 1, line 62). Anshel et al. describe generating a key split from maintenance data (see "s = 1, 2, 3, . . . denote the state of the user" in column 8, lines 8-15). Albert et al. disclose a random number generating system that picks, at a random point in time, a value from another system generating different random numbers as a function of time (see column 1, lines 51-67 and column 2, lines 1-2). This can readily be combined with random key split generator based on maintenance data of Hirsch in view of Anshel et al.

As per claims 25-31 and 59- 65, as stated above, Hirsch describes the randomizer for combining key splits (see column 1, lines 54-58). Tomko et al. elaborate on a biometric split generator for generating a biometric key split based on biometric data (see column 2, lines 2-20).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it is obvious to combine these references to have secure, yet readily available private key (see column 1, lines 58-60).

As per claims 31 and 65, Tomko et al. elaborate on static data (see "w is a constant for any specified number of peaks (t)" in column 7, line 46). In a specific embodiment, Tomko et al. suggest that the number of peaks is 4 (see figure 3 and column 9, lines 29-32). As a result of this, the expression for "w" (see column 8, lines 11-12) has a prime number divisor, (t-1), of 3.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 2, 4, 32, 33, 34, 35, 36, 38, 67, 68, and 69 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Hirsch, U.S. Patent No. 5,276,738.

As per claims 1, 35, and 66, Hirsch illustrates a cryptographic key split combiner, a process for combining, and a key formed by the process comprising: a plurality of key split generators for generating cryptographic key splits (see column 1, lines 57-67); and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key (see column 1, lines 54-57 and lines 62-68; column 2, lines 1-7; column 3, lines 60-65; and figure 1A, items 10, 12, and 16); in which each of the key split generators includes means for generating key splits from seed data (see column 1, lines 49-54 and lines 62-64).

As per claims 2 and 36, Hirsch further teaches that the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 55-58).

As per claims 4 and 38, Hirsch then suggests that the random split generator includes means for generating a pseudorandom sequence based on the reference data (see column 2, lines 23-29).

As per claims 32 and 67, Hirsch moreover discusses that the cryptographic key is a stream of symbols (see column 4, lines 33-44).

As per claims 33 and 68, Hirsch next describes that the key is at least one symbol block (see column 4, lines 38-40).

As per claims 34 and 69, Hirsch subsequently specifies that the cryptographic key is a key matrix (see column 2, lines 5-7).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 as applied to claim 2 above, and further in view of Albert et al., U.S. Patent No. 5,627,894.

Hirsch teaches the cryptographic key split combiner and process of combining of claim 2. Although he describes that the random key split generator includes means for generating a pseudorandom sequence based on reference data (see column 2, lines 23-29), he does not explicitly mention generating a random sequence. Albert et al. specify generating a random sequence (see column 1, lines 51-67 and column 2, lines 1-2). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with generating a random sequence of Albert et al. to increase the quality of random numbers with respect to their predictability and their functional link (see column 1, lines 66-67 and column 2, lines 1-2).

9. Claims 5 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 as applied to claim 2 above, and further in view of Thomlinson et al., U.S. Patent No. 5,778,069.

Hirsch teaches the cryptographic key split combiner and process of combining of claim 2. However, he does not explicitly show chronological data. Thomlinson et al. disclose generating a key split based on reference data and on chronological data (see column 3, lines 16-23). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with generating a key split based on chronological data of Thomlinson et al. to ensure unguessability (see column 3, lines 2-7).

10. Claims 6, 7, 9, 10, 11, 13, 14, 15, 16, 40, 41, 43, 44, 45, 47, 48, 49, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 as applied to claim 2 above, and further in view of Ming et al., U.S. Patent No. 5,710,815.

As per claims 6 and 40, Hirsch explain the cryptographic key split combiner and process of combining of claim 2. However, he does not explicitly delineate static data. Ming et al. discuss generating a key split based on reference data and on static data (see column 4, lines 4-7). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with generating a key split based on static data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10).

As per claims 7 and 41, Ming et al. further disclose a means of updating the static data (see column 4, line 8). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with updating static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4).

As per claims 9 and 43, Ming et al. then discuss a token split generator for generating a token key split based on label data (see column 6, lines 26-29; column 5, lines 65-67; column 6, lines 1-5; and column 10, lines 27-34). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with the token split generator of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10).

As per claims 10 and 44, Ming et al. moreover suggest reading the label data from a storage medium (see column 7, lines 11-22). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with reading the label data from a storage medium of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10).

As per claims 11 and 45, Ming et al. next describe that the label data includes user authorization data (see column 7, lines 11-22). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with user authorization data as label data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10).

As per claims 13 and 47, Ming et al. also illustrate a means for generating a pseudorandom sequence based on label data (see column 13, lines 45-50; figure 2, items 113-115; column 14, lines 39-44; and column 15, lines 40-60). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with the means for generating a pseudorandom sequence based on label data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10).

As per claims 14 and 48, Ming et al. subsequently specify the means for generating a key split based on label data and on organization data (see column 6, lines 26-29 and lines 59-65; column 5, lines 65-67; and column 6, lines 1-5). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with the means for generating a key split based on label data and on organization data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10).

As per claims 15 and 49, Ming et al. then suggest a means for generating a key split based on the label data and on static data (see column 4, lines 4-7). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with the means for generating a key split based on the label data and on static data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10).

As per claims 16 and 50, Ming et al. moreover describe a means for updating the static data. Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with the means for updating the static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4).

11. Claims 8 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 in view of Ming et al., U.S. Patent No. 5,710,815 as applied to claim 7 above, and further in view of Anshel et al., U.S. Patent No. 5,751,808.

Hirsch in view of Ming et al. teaches the cryptographic key split combiner and process for combining of claim 7. Ming et al. describe modifying a divisor of the static data (see column 4, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Ming et al. with modifying a divisor of the static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines

65-67 and column 4, lines 1-4). However, Ming et al. do not specify that this value is a prime divisor. Anshel et al. show modifying a prime divisor of the static data (see column 11, lines 8-25 and figure 8, item 71). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Ming et al. with modifying a prime divisor of the static data of Anshel et al. to generate a cryptographically secure sequence at high speed (see column 1, lines 11-12).

12. Claims 12 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 in view of Ming et al., U.S. Patent No. 5,710,815 as applied to claim 7 above, and further in view of Albert et al., U.S. Patent No. 5,627,738.

Hirsch in view of Ming et al. teach the cryptographic key split combiner and process for combining of claim 9. Ming et al. illustrate a means for generating a pseudorandom sequence based on label data (see column 13, lines 45-50; figure 2, items 113-115; and column 14, lines 39-44). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Ming et al. with generating a pseudorandom sequence based on label data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10). However, neither Hirsch nor Ming et al. specify that this is a random sequence. Albert et al. elaborate on generating a random sequence (see column 1, lines 51-67 and column 2, lines 1-2). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Ming et al. with generating a random sequence of Albert et al. to increase the quality of random numbers with respect to their predictability and their functional link (see column 1, lines 66-67 and column 2, lines 1-2).

13. Claims 17 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 in view of Ming et al., U.S. Patent No. 5,710,815 as applied to claim 7 above, and further in view of Anshel et al., U.S. Patent No. 5,751,808.

Hirsch in view of Ming et al. teach the cryptographic key split combiner and process for combining of claim 16. Ming et al. describe modifying a divisor of the static data (see column 4, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Ming et al. with modifying a divisor of the static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4). However, Ming et al. do not specify that this value is a prime divisor. Anshel et al. show modifying a prime divisor of the static data (see column 11, lines 8-25 and figure 8, item 71). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Ming et al. with modifying a prime divisor of the static data of Anshel et al. to generate a cryptographically secure sequence at high speed (see column 1, lines 11-12).

14. Claims 18, 20, 21, 22, 23, 24, 52, 54, 55, 56, 57, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 as applied to claim 1 above, and further in view of Anshel et al., U.S. Patent No. 5,751,808.

As per claims 18 and 52, Hirsch teaches the cryptographic key split combiner and process for combining of claim 1. However, he does not describe maintenance data. Anshel et al. discuss a console split generator for generating a console key split based on maintenance data (see column 8, lines 8-15). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with generating a console key split based on maintenance data of Anshel et al. for simple and highly secure authentication (see column 8, lines 8-9).

As per claims 20 and 54, Anshel et al. then describe a means for generating a pseudorandom sequence based on maintenance data (see column 8, lines 8-15). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with a means for generating a pseudorandom sequence based on maintenance data of Anshel et al. for simple and highly secure authentication (see column 8, lines 8-9).

As per claims 21 and 55, Anshel et al. further specify generating a key split based on previous maintenance data and on current maintenance data (see column 8, lines 26-27).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with generating a key split based on previous maintenance data and on current maintenance data of Anshel et al. for simple and highly secure authentication (see column 8, lines 8-9).

As per claims 22 and 56, Anshel et al. moreover mention generating a key split based on the maintenance data and on static data (see column 8, lines 16-22). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with generating a key split based on maintenance data and on static data of Anshel et al. for simple and highly secure authentication (see column 8, lines 8-9).

As per claims 23 and 57, Anshel et al. subsequently delineate a means for updating the static data (see column 8, lines 8 and 26-27). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with updating the static data of Anshel et al. to generate a cryptographically secure sequence at high speed (see column 1, lines 11-12).

As per claims 24 and 58, Anshel et al. next illustrate updating the static data includes modifying a prime number divisor of the static data (see column 11, lines 8-25 and figure 8, item 71). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with modifying a prime number divisor of the static data of Anshel et al. to generate a cryptographically secure sequence at high speed (see column 1, lines 11-12).

15. Claims 19 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 in view of Anshel et al., U.S. Patent No. 5,751,808 as applied to claim 18 above, and further in view of Albert et al., U.S. Patent No. 5,627,738.

Hirsch in view of Anshel et al. disclose the cryptographic key split combiner and process of combining of claim 18. Anshel et al. describe a means for generating a pseudorandom sequence based on maintenance data (see column 8, lines 8-15). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Anshel et al. with a means for generating a pseudorandom sequence of Anshel et al. for very simple and highly secure authentication (see column 8, lines 8-9). However, they do not explicitly teach a random sequence. Albert et al. specify a random sequence (see column 1, lines 51-67 and column 2, lines 1-2). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Anshel et al. with a means for generating a random sequence of Albert et al. to increase the quality of random numbers with respect to their predictability and their functional link (see column 1, lines 66-67 and column 2, lines 1-2).

16. Claims 25, 27, 28, 29, 30, 31, 59, 61, 62, 63, 64, and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 as applied to claim 1 above, and further in view of Tomko et al., U.S. Patent No. 5,541,994.

As per claims 25 and 59, Hirsch teaches the cryptographic key split combiner and process of combining of claim 1. However, he does not suggest generating a biometric key split based on biometric data. Tomko et al. elaborate on a biometric split generator for generating a biometric key split based on biometric data (see column 2, lines 2-20). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with a biometric split generator for generating a biometric key split based on biometric data of Tomko et al. to have secure, yet readily available private key (see column 1, lines 58-60).

As per claims 27 and 61, Tomko et al. further disclose a means for generating a pseudorandom sequence based on the biometric data (see column 2, lines 2-12). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with a means for generating a pseudorandom sequence based on the biometric data of Tomko et al. to have secure, yet readily available private key (see column 1, lines 58-60).

As per claims 28 and 62, Tomko et al. next delineate a means for generating a key split based on biometric data vectors and on biometric combiner data (see column 3, lines 56-67). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with a means for generating a key split based on biometric data vectors and on biometric combiner data of Tomko et al. to have secure, yet readily available private key (see column 1, lines 58-60).

As per claims 29 and 63, Tomko et al. moreover explain a means for generating a key split based on biometric data and on static data (see column 3, lines 56-67). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with a means for generating a key split based on biometric data and on static data of Tomko et al. to have secure, yet readily available private key (see column 1, lines 58-60).

As per claims 30 and 64, Tomko et al. then illustrate updating the static data (see column 7, lines 33-39 and figure 1, items 43 and 44). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with updating the static data of Tomko et al. for enrolling an individual (see column 7, lines 33-36).

As per claims 31 and 65, Tomko et al. further elaborate on the means for updating the static data includes means for modifying a prime number divisor of the static data (see column 7, lines 45-67 and column 8, lines 1-12). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch with a means for modifying a prime number divisor of the static data of Tomko et al. so that the subscriber can later reproduce the static data (see column 8, lines 22-24).

17. Claims 26 and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirsch, U.S. Patent No. 5,276,738 in view of Tomko et al., U.S. Patent No. 5,541,994 as applied to claim 25 above, and further in view of Albert et al., U.S. Patent No. 5,627,738.

Hirsch in view of Tomko et al. disclose the cryptographic key split combiner and process of combining of claim 25. Tomko et al. discuss a means for generating a pseudorandom sequence based on the biometric data (see column 2, lines 2-12). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Tomko et al. with a means for generating a pseudorandom sequence based on the biometric data of Tomko et al. to have secure, yet readily available private key (see column 1, lines 58-60). However, they do not explicitly teach a random sequence. Albert et al. specify a random sequence (see column 1, lines 51-67 and column 2, lines 1-2). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the cryptographic key split combiner and process of combining of Hirsch in view of Tomko et al. with a means for generating a random sequence of Albert et al. to increase the quality of random numbers with respect to their predictability and their functional link (see column 1, lines 66-67 and column 2, lines 1-2).

Conclusion

18. This is a request for continued examination of applicant's earlier Application No. 09/023,672. All claims are drawn to the same invention claimed in the earlier application and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the earlier application. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action in this case. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no, however, event will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872. The examiner can normally be reached Monday-Friday from 8:00 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod R. Swann, can be reached at (703) 308-7791.

The fax number for Formal or Official faxes to Technology Center 2700 is (703) 308-9051 or 9052. Draft or Informal faxes for this Art Unit can be submitted to (703) 305-0040.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

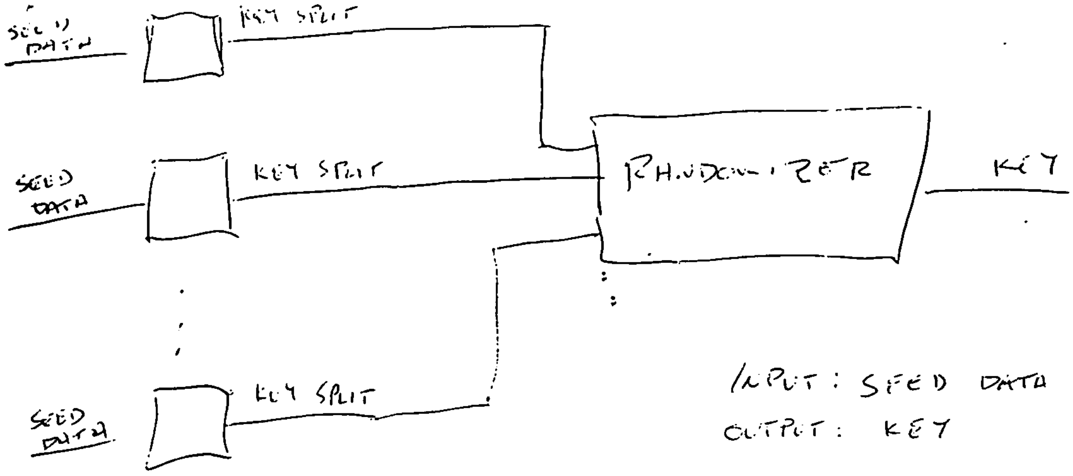
TOD R. SWANN
SUPERVISORY PATENT EXAMINER
GROUP 2700

Justin T. Darrow

July 20, 2000

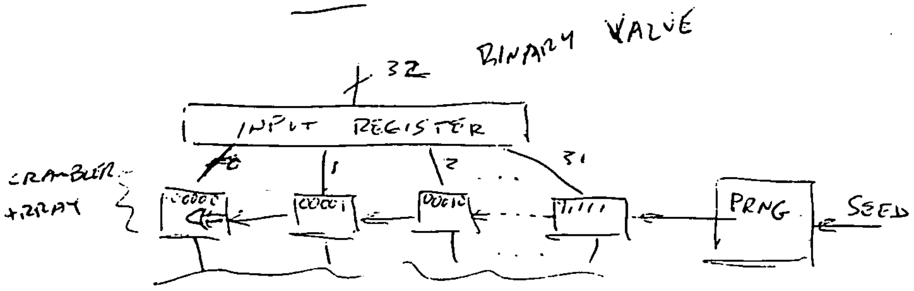
CLAIM 1:

KEY SPLIT GENERATORS



INPUT: SEED DATA
OUTPUT: KEY

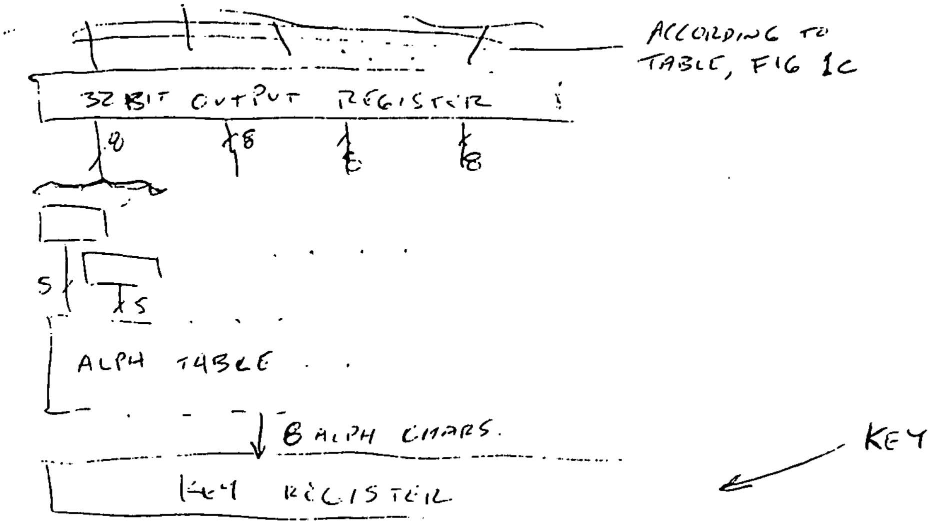
HIRSCH



INPUT: 32-BIT BINARY VALUE
SEED

EACH INPUT BIT GOES TO
AN ARRAY CONTAINER
5-BIT RANDOM # SHIFTED IN FROM PRNG
RANDOM # XOR W/ BIT POSITION
LSB OF RESULT DETERMINES IF
INPUT BIT OR COMPLEMENT IS THE
OUTPUT OF THE CONTAINER

FIG 1A


ACCORDING TO TABLE, FIG 1C
32 BIT OUTPUT REGISTER
8
8
8
8
5
5
ALPH TABLE
8 ALPH CHARS.
KEY REGISTER
KEY